## REPLACEMENT CLAIMS

## 1-12 Cancel

13. (currently amended) The method of Claim 7, wherein said filtering conditions include A method for controlling e-mail message transmission across an e-mail firewall, the e-mail firewall interposed between an internal network associated with a first policy and an external network, the method comprising:

intercepting a plurality of data packets associated with a message
from a sender user associated with the internal network, the message
directed to a recipient user associated with an external network;
assembling said data packets to an application level message;
filtering the application level message by examining textual
content associated with the application level message by employing
content filter conditions of the first policy to provide a filtering result;
requiring executable attachments to include digital signatures; and
restricting the transmission of the application level message in
accordance with said filtering result.

- 14. (original) The method Claim 13, further comprising filtering executable attachments by reference to a directory of trusted signatures.
- 15. (original) The method of Claim 13, wherein said restricting the transmission includes routing the message in accordance with user defined routing policies.

  16-28 (Canceled)

- 29. (previously presented) A method for filtering e-mail messages transmitted from an external site to an internal site associated with a first policy, comprising:
  - i. intercepting a plurality of data packets associated with an e-mail message having a sender address associated with an external site;
  - ii. assembling said data packets to an application level message;
  - iii. detecting whether the application level message includes a digital signature attachment;
  - iv. applying at least one policy condition to said application level email message, said policy condition applied by reference to said attached digital signature, said applying providing a policy application result; and
  - v. processing said application level e-mail message in accordance with said application result.
- 30. (previously presented) The method of Claim 29, further comprising applying at least a second policy condition to said application level e-mail message in response to a predetermined condition of the attached digital signature.
- 31. (previously presented) The method of Claim 30, wherein said predetermined condition comprises detecting that the digital signature is a valid digital signature.
- 32. (previously presented) The method of Claim 31, further comprising selecting the second policy condition by reference to an identity associated with the valid digital signature.
- 33. (previously presented) the method of Claim 30, wherein the second policy condition detects whether the attached signature is associated with a domain which is included in a stored list of trusted domains.